REMARKS

The Office Action dated October 31, 2008 has been received and carefully noted. The above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto.

Claims 1 and 4-12 have been amended to more particularly point out and distinctly claim the subject matter of the invention. Claim 2 has been cancelled without prejudice or disclaimer. New claims 13-18 have been added. No new matter has been added. Therefore, claims 1 and 3-18 are currently pending in the application and are respectfully submitted for consideration.

Claim Rejections Under 35 U.S.C. § 103(a)

The Office Action rejected claims 1-12 under 35 U.S.C. § 103(a) as allegedly being unpatentable over Poeluev (U.S. Patent No. 7,366,794) ("Poeluev"), in view of Buddhikot et al. (U.S. Publication No. 2005/0013280) ("Buddhikot"), and further in view of Bahl et al. (U.S. Publication No. 2003/0069016) ("Bahl"). The Office Action took the position that Poeluev discloses all the elements of the claims with the exception of "the mobile terminal has a second address that identifies the mobile terminal in the second network," "in the security gateway, identifying the secure tunnel based on the second address in packets destined for the mobile terminal from the second network," "detecting a change in the first address of the mobile terminal," "in response to the detecting step, sending an update message to the security gateway, wherein the update message includes

a new address value of the first address," "based on the update message, updating the first address associated with the secure tunnel." The Office Action then cited Buddhikot and Bahl as allegedly curing the deficiencies of Poeluev.

Applicants respectfully submit that claim 2 has been cancelled, and said cancellation effectively moots the rejection, with respect to claim 2. With respect to the remaining claims, Applicants respectfully submit that said claims recite allowable subject matter for at least the following reasons.

Claim 1, upon which claims 3-5 are dependent, recites a method, which includes establishing a secure tunnel between a security gateway in a second network and a mobile terminal located at a first address in a first network, where the first network is a public packet network and the second network is a private packet network, the security gateway connects the first network to a second network, and the mobile terminal has a second address that identifies the mobile terminal in the second network. The method further includes in the security gateway, identifying the secure tunnel based on the second address in packets destined for the mobile terminal from the second network, and detecting a change in the first address of the mobile terminal. The method further includes in response to the detecting, sending an update message to the security gateway, wherein the update message includes a new address value of the first address, and based on the update message, updating the first address associated with the secure tunnel.

Claim 6 recites an apparatus, which includes tunnel establishment means for establishing a secure tunnel to a security gateway through a packet network, where the

security gateway is configured to connect a first network to a second network, the first network being a public packet network and the second network being a private packet network, the security gateway is in the second network and the mobile terminal has a first address that depends on its current location in the first network and a second address that identifies the mobile terminal in the second network. The apparatus further includes address update means for sending an update message through said secure tunnel to the security gateway when the first address changes, wherein the update message includes a new address value of the first address.

Claim 9 recites an apparatus, which includes tunnel establishment means for establishing a secure tunnel to a mobile terminal located at a first address in a first network, where the security gateway is in a second network and configured to connect the first network to a second network, the first network being a public packet network and the second network being a private packet network, and the mobile terminal has a second address that identifies the mobile terminal in the second network. The apparatus further includes identification means for identifying the secure tunnel based on the second address in a packet originated from the second network and destined for the mobile terminal. The apparatus further includes address update means for updating the first address associated with the secure tunnel, the address update means being responsive to a message received from the mobile terminal, the message including a new value of the first address.

Claim 10 recites a system, which includes tunnel establishment means for establishing a secure tunnel between a security gateway in a second network and a mobile terminal located at a first address in a first network, where the first network is a public packet network and the second network is a private packet network, the security gateway is configured to connect the first network to a second network, and the mobile terminal has a second address that identifies the mobile terminal in the second network. The system further includes detection means for detecting a change in the first address. The system further includes first address update means, responsive to the detection means, for sending an update message to the security gateway, wherein the update message includes a new address value of the first address. The system further includes, in the security gateway, second address update means for updating the first address associated with the secure tunnel in response to the update message, and, in the security gateway, identification means for identifying the secure tunnel based on the second address in a packet originated from the second network and destined for the mobile terminal.

Claim 11 recites a computer useable storage medium having computer readable program code embodied therein to enable a mobile terminal to communicate with a security gateway in a packet-based communication system. The computer readable program code includes computer readable program code configured to cause the mobile terminal to establish a secure tunnel to a security gateway through a packet network, where the security gateway is configured to connect a first network to a second network, the first network being a public packet network and the second network being a private

packet network, the security gateway is in the second network, and the mobile terminal has a first address that depends on its current location in the first network and a second address that identifies the mobile terminal in the second network. The computer readable program code further includes computer readable program code configured to cause the mobile terminal to send an update message through said secure tunnel to the security gateway when the first address changes, where the update message includes a new address value of the first address.

Claim 12 recites a computer useable medium having computer readable program code embodied therein to enable a mobile terminal located at a first address in a first network to communicate with a security gateway in a packet-based communication system, the security gateway being in a second network and configured to connect a first network to a second network, the first network being a public packet network and the second network being a private packet network. The computer readable program code includes computer readable program code configured to cause the mobile terminal to send an update message through a secure tunnel to the security gateway when a first address that depends on the mobile terminal's current location in the first network changes, wherein the update message includes a new address value of the first address.

Claim 13 recites a method, which includes establishing a secure tunnel from a first network to a security gateway in a second network through a packet network; where the security gateway is configured to connect a first network to a second network, the first network is a public packet network and the second network is a private packet network,

and the mobile terminal has a first address that depends on its current location in the first network and a second address that identifies the mobile terminal in the second network. The method further includes sending an update message through said secure tunnel to the security gateway when the first address changes, wherein the update message includes a new address value of the first address.

Claim 14 recites a method, which includes establishing a secure tunnel from a second network to a mobile terminal located at a first address in a first network, where the security gateway is configured to connect the first network to a second network, the first network is a public packet network and the second network is a private packet network, and the mobile terminal has a second address that identifies the mobile terminal in the second network. The method further includes identifying the secure tunnel based on the second address in a packet originated from the second network and destined for the mobile terminal. The method further includes updating the first address associated with the secure tunnel, the address update means being responsive to a message received from the mobile terminal, the message including a new value of the first address.

Claim 15 recites an apparatus, which includes a control unit configured to establish a secure tunnel from a first network to a security gateway in a second network through a packet network; where the security gateway is configured to connect a first network to a second network, the first network is a public packet network and the second network is a private packet network, and the mobile terminal has a first address that depends on its current location in the first network and a second address that identifies

the mobile terminal in the second network. The control unit is further configured to send an update message through said secure tunnel to the security gateway when the first address changes, wherein the update message includes a new address value of the first address.

Claim 16 recites an apparatus, which includes a control unit configured to establish a secure tunnel from a second network to a mobile terminal located at a first address in a first network, where the security gateway is configured to connect the first network to a second network, the first network is a public packet network and the second network is a private packet network and the mobile terminal has a second address that identifies the mobile terminal in the second network. The control unit is further configured to identify the secure tunnel based on the second address in a packet originated from the second network and destined for the mobile terminal, and update the first address associated with the secure tunnel, being responsive to a message received from the mobile terminal, the message including a new value of the first address.

As will be discussed below, the combination of Poeluev, Buddhikot, and Bahl fails to disclose or suggest all of the elements of the claims, and therefore fails to provide the features discussed above.

Poeluev discloses a network 10 which includes a public network 12 and a virtual private network (VPN 14). The public network 12 includes an Internet service provider (ISP 16) along with an ISP domain server (DNS 18). A public host 20 may be connected to the Internet 22 via the ISP 16. The public host 20 may also be connected to the VPN

14 via a VPN tunnel 22 or via the public network 12. In both cases, the public host 20 is connected to a security gateway 24 associated with the VPN 14 which requires the public host to log on to the VPN 14. The VPN 14 includes a VPN DNS 26 as well as address locations (i.e. private hosts) 28 which are not accessible via the public network 12. (See Poeluev at col. 2, lines 53-67; Figure 1).

Buddhikot discloses a Mobile NAT (mobile network address translation) device which receives packets identifying a virtual IP address of a mobile node coupled to the Mobile NAT as a destination. The Mobile NAT identifies an actual IP address of the mobile node based on the virtual IP address. The Mobile NAT associates a second actual IP address of the mobile node with the same virtual IP address when the Mobile NAT is notified that the mobile node is moving. The Mobile NAT routes the packets to the mobile node via an IP-in-IP tunnel, using the first IP address when the mobile node is in the first subnet and the second IP address when the mobile node is in the second subnet. (See Buddhikot at paragraphs 0012 and 0056).

Bahl discloses a system and method for mobility support which handles address changes of a mobile host. When the mobile host changes to a new address, the mobile host sends an address change message to each of its correspondent hosts over a control channel. Upon receiving the notification, the correspondent host returns an acknowledgment through the control channel and notifies its security filters and transport control parameters corresponding to the connection with the mobile host to use the new address. After receiving the acknowledgment, the mobile host modifies its security filters

and transport control parameters for the connection to use the new address. (See Bahl at Abstract).

Applicants respectfully submit that Poeluev, Buddhikot, and Bahl, whether considered individually or in combination, fail to disclose, teach, or suggest, all of the elements of the present claims. For example, the combination of Poeluev, Buddhikot, and Bahl fails to disclose, teach, or suggest, at least:

- "*establishing a secure tunnel between a security gateway in a second network and a mobile terminal located at a first address in a first network, wherein the first network is a public packet network and the second network is a private packet network and the security gateway connects the first network to a second network,*" and "*in the security gateway, identifying the secure tunnel based on the second address in packets destined for the mobile terminal from the second network,*" as recited in independent claim 1;
- "*tunnel establishment means for establishing a secure tunnel to a security gateway through a packet network; wherein the security gateway is configured to connect a first network to a second network, the first network being a public packet network and the second network being a private packet network,*" as recited in independent claim 6;
- "*tunnel establishment means for establishing a secure tunnel to a mobile terminal located at a first address in a first network, wherein the security gateway is in a second network and configured to connect the first network to a second network,*

the first network being a public packet network and the second network being a private packet network," and "*identification means for identifying the secure tunnel based on the second address in a packet originated from the second network and destined for the mobile terminal*," as recited in independent claim 9;

- "*tunnel establishment means for establishing a secure tunnel between a security gateway in a second network and a mobile terminal located at a first address in a first network, wherein the first network is a public packet network and the second network is a private packet network, the security gateway is configured to connect the first network to a second network*," and "*in the security gateway, identification means for identifying the secure tunnel based on the second address in a packet originated from the second network and destined for the mobile terminal*," as recited in independent claim 10;
- "*computer readable program code configured to cause the mobile terminal to establish a secure tunnel to a security gateway through a packet network; wherein the security gateway is configured to connect a first network to a second network, the first network being a public packet network and the second network being a private packet network*," as recited in independent claim 11;
- "*computer readable program code embodied therein to enable a mobile terminal located at a first address in a first network to communicate with a security gateway in a packet-based communication system, the security gateway being in a second network and configured to connect a first network to a second network, the*

first network being a public packet network and the second network being a private packet network," as recited in independent claim 12;

- "*establishing a secure tunnel from a first network to a security gateway in a second network through a packet network; wherein the security gateway is configured to connect a first network to a second network, the first network is a public packet network and the second network is a private packet network*," as recited in independent claim 13;
- "*establishing a secure tunnel from a second network to a mobile terminal located at a first address in a first network, wherein the security gateway is configured to connect the first network to a second network, the first network is a public packet network and the second network is a private packet network*," and "*identifying the secure tunnel based on the second address in a packet originated from the second network and destined for the mobile terminal*," as recited in independent claim 14;
- "*a control unit configured to establish a secure tunnel from a first network to a security gateway in a second network through a packet network; wherein the security gateway is configured to connect a first network to a second network, the first network is a public packet network and the second network is a private packet network*," as recited in independent claim 15; and
- "*a control unit configured to establish a secure tunnel from a second network to a mobile terminal located at a first address in a first network, wherein the security gateway is configured to connect the first network to a second network, the first*

network is a public packet network and the second network is a private packet network," as recited in independent claim 16.

With respect to "*establishing a secure tunnel between a security gateway in a second network and a mobile terminal located at a first address in a first network, wherein the first network is a public packet network and the second network is a private packet network and the security gateway connects the first network to a second network*," as recited in independent claim 1, the Office Action took the position that Poeluev discloses the aforementioned limitation at col. 2, lines 15-23 and 53-65; Figure 1. (See Office Action at page 2). Applicants respectfully submit that the Office Action is incorrect because the cited portion of Poeluev fails to disclose, or suggest, a mobile terminal in a first (i.e. public packet) network and a security gateway in a second (i.e. private packet) network. Specifically, Poeluev merely identifies that a public network includes an ISP 16 and that a public host 20 may be connected to the Internet 22 via the ISP 16. (See Poeluev at col. 2, lines 57-58). However, Poeluev fails to disclose, or suggest, that the public host 20 is a mobile terminal. In fact, Poeluev specifically identifies the connection between the public host 20 and the Internet 22, via the ISP 16, as a wired connection. Specifically, Poeluev discusses that the connection between the public host and the ISP is via a dial-up connection, or a direct Ethernet connection. (See Poeluev at col. 3, lines 1-5). Thus, the cited portion of Poeluev fails to disclose, or suggest, a mobile terminal in a first (i.e. public packet) network.

Similarly, Poeluev fails to disclose, or suggest, a security gateway in a second (i.e. private packet) network. Specifically, Poeluev merely identifies a security gateway 24 which is associated with a VPN 14. (See Poeluev at col. 2, lines 60-62). The cited portion of Poeluev fails to explicitly disclose that the security gateway 24 is within the VPN 14.

Furthermore, Buddhikot does not cure the deficiencies of Poeluev. As described above, Buddhikot merely discloses a Mobile NAT routing packets via an IP-in-IP tunnel from an anchor node to a mobile node. However, the IP-in-IP tunnel identified in Buddhikot is a tunnel between elements in the same NAT domain, and is not a tunnel which connects two separate networks.

Additionally, the IP-in-IP tunnel of Buddhikot is not a secure tunnel. In a secure tunnel, the integrity of the delivered information is, by definition, secured and becomes available when the tunnel is successful identified. The cited portion of Buddhikot fails to disclose, or suggest, security-related protocols for the tunnel between the anchor node and the mobile node.

Buddhikot also fails to disclose, or suggest, a secure gateway. Instead, Buddhikot merely discloses that the translation from actual IP to virtual IP occurs at the anchor node, and that the anchor node is a mere standard NAT or NAPT device. (See Buddhikot at paragraph 0053). The cited portion of Buddhikot fails to disclose, or suggest, that the anchor node engages in any specific security procedures.

Finally, Bahl does not cure the deficiencies of Poeluev and Buddhikot. As described above, Bahl merely discloses sending an address change message from a mobile host to a correspondent host to change the address of a mobile host. The cited portion of Bahl fails to discuss a first network and a second network where the first network is a public packet network and the second network is a private packet network. Thus, the cited portion of Bahl fails to disclose, or suggest, establishing a secure tunnel between a security gateway in a second network and a mobile terminal located at a first address in a first network, wherein the first network is a public packet network and the second network is a private packet network and the security gateway connects the first network to a second network.

Thus, Poeluev, Buddhikot, and Bahl, whether considered individually or in combination, fails to disclose, or suggest, "*establishing a secure tunnel between a security gateway in a second network and a mobile terminal located at a first address in a first network, wherein the first network is a public packet network and the second network is a private packet network and the security gateway connects the first network to a second network*," as recited in independent claim 1. Furthermore, Applicants respectfully submit that, while independent claims 6 and 9-16 each have their own scope, each recites a limitation similar to the aforementioned limitation of independent claim 1, and thus, the arguments presented above also apply to independent claims 6 and 9-16.

With respect to "*in the security gateway, identifying the secure tunnel based on the second address in packets destined for the mobile terminal from the second network*," as

recited in independent claim 1, the Office Action correctly concluded that Poeluev fails to disclose, or suggest, the aforementioned limitation. (See Office Action at page 2). Furthermore, Buddhikot does not cure the deficiencies of Poeleuv. As discussed above, the cited portion of Buddhikot is silent as to a secure tunnel. Accordingly, the cited portion of Buddhikot is also silent as to identifying a secure tunnel. Furthermore, as also discussed above, Buddhikot is also silent as to a secure tunnel between a first network and a second network, as Buddhikot merely discloses a tunnel between elements in the same NAT domain.

Finally, Bahl does not cure the deficiencies of Poeluev and Buddhikot. As described above, Bahl merely discloses sending an address change message from a mobile host to a correspondent host to change the address of a mobile host. Thus, the cited portion of Bahl fails to disclose, or suggest identifying the secure tunnel based on the second address in packets destined for the mobile terminal from the second network.

Thus, Poeluev, Buddhikot, and Bahl, whether considered individually or in combination, fails to disclose, or suggest, "*in the security gateway, identifying the secure tunnel based on the second address in packets destined for the mobile terminal from the second network*," as recited in independent claim 1. Furthermore, Applicants respectfully submit that, while independent claims 9-10 and 14 each have their own scope, each recites a limitation similar to the aforementioned limitation of independent claim 1, and thus, the arguments presented above also apply to independent claims 9-10 and 14.

Therefore, for at least the reasons discussed above, the combination of Poeluev, Buddhikot, and Bahl fails to disclose, teach, or suggest, all of the elements of independent claims 1, 6, and 9-16.

Furthermore, as an **alternative** basis for traversing the rejection, Applicants respectfully submit that the Office Action has failed to establish a prima facie case that independent claims 1, 6 and 9-16 are obvious in light of Poeluev, Buddhikot, and Bahl, because Buddhikot is not analogous art.

As reiterated by the Supreme Court in *KSR International Co. v. Teleflex Inc.*, 550 U.S. ___, 82 USPQ2d 1385 (2007), the framework for the objective analysis for determining obviousness under 35 U.S.C. § 103 is stated in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966). Obviousness is a question of law based on underlying factual inquiries. The factual inquiries are: (a) determining the scope and content of the prior art; (b) ascertaining the differences between the claimed invention and the prior art; and (c) resolving the level of ordinary skill in the pertinent art. (see *KSR International Co. v. Teleflex Inc.*, 550 U.S. ___, 82 USPQ2d 1385 (2007); *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966); see also MPEP 2141).

For a reference to be used in an obviousness rejection, the reference must be in an analogous field to that of the invention; in other words, the reference must either be in the field of the inventor's endeavor or reasonably pertinent to the specific problem with which the inventor was involved. (See *In re Deminski*, 796 F.2d 436, 442, 230 USPQ 313, 315 (Fed. Circ. 1986)).

As discussed above, Buddhikot merely discloses a Mobile NAT routing packets via an IP-in-IP tunnel from an anchor node to a mobile node, where the IP-in-IP tunnel is a tunnel between elements in the same NAT domain, and is not a tunnel which connects two separate networks. In contrast, certain embodiments of the invention are directed towards establishing a secure tunnel between a first private network and a second public network. Thus, one of ordinary skill in the art would not combine the reference of Buddhikot with the reference of Poeluev as the configuration and definition of tunnel in Buddhikot is incompatible with the configuration and definition of tunnel in Poeluev, and the concepts are not applicable to each other.

Therefore, for at least the reasons stated above, the Office Action has failed to establish a prima facie case that independent claims 1, 6 and 9-16 are obvious in light of the cited references of Poeluev, Buddhikot, and Bahl.

For the reasons stated above, Applicants respectfully request that this rejection be withdrawn.

Claims 3-5 depend upon independent claim 1. Claims 7-8 depend upon independent claim 15. Claims 17-18 depend upon independent claim 16. Thus, Applicants respectfully submit that claims 2-5, 7-8, and 17-18 should be allowed for at least their dependence upon independent claims 1 and 15-16, and for the specific elements recited therein.

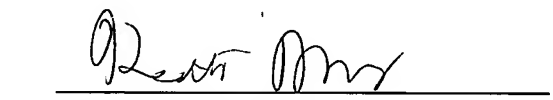
For at least the reasons discussed above, Applicants respectfully submit that the cited prior art references fail to disclose or suggest all of the elements of the claimed

invention. These distinctions are more than sufficient to render the claimed invention unanticipated and unobvious. It is therefore respectfully requested that all of claims 1 and 3-18 be allowed, and this application passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicants undersigned representative at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicant respectfully petitions for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,



Keith M. Mullervy
Registration No. 62,382

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Vienna, Virginia 22182-6212
Telephone: 703-720-7800
Fax: 703-720-7802

KMM:sew

Enclosures: Additional Claim Fee Transmittal
Check No. 20368 ($880.00)